ANÁLISIS SISTEMÁTICO DE LA SEGURIDAD EN INTERNET OF THINGS

Mg. Ing. Norma Beatriz Perez[(1)], Miguel Alfredo Bustos[(1)(*)], Dr. Mario M. Berón[(1)] & PhD. Pedro Rangel Henriques[(2)]

[(1)]Departamento de Informática - Facultad de Ciencias Física Matemáticas y Naturales (FCFMyN) - Universidad Nacional de San Luis

[(2)]Universidade do Minho - Braga, Portugal

{nbperez, mabustos, mberon}@unsl.edu.ar[(1)], pedrorangelhenriques@gmail.com[(2)]

(*) Estudiante de la Carrera de Ingeniería en Informática

RESUMEN

Internet of Things (IoT, siglas en inglés) es una innovación tecnológica con gran auge en la actualidad debido a la incorporación en múltiples sectores en la sociedad como en la salud (Smart Health), en la educación (Smart Education), en el hogar (Smart Home), en el transporte (Smart Transport), en la seguridad (Smart Segurity), en las ciudades (Smart City), entre otros sectores. IoT permite interconectar objetos integrados físicos (Smart Object) en diferentes redes de comunicación transmitiendo y recibiendo información. Sin embargo, debido a su evolución exponencial surge la problemática de la seguridad y privacidad que afecta directamente en el desarrollo y mantenimiento de la utilización sostenible de IoT.

En este trabajo se describe la línea de investigación que aborda el estudio y análisis de seguridad en IoT. Dicho estudio se fundamenta en el análisis de la seguridad en las diferentes capas de la arquitectura de la misma.

Palabras Claves: Internet of Things, Objetos Físicos, Seguridad en IoT, Arquitectura IoT.

CONTEXTO

La presente línea de investigación se enmarca en el Proyecto (PO/16/93) de *"Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa"*. Realizado en conjunto con la Universidade do Minho Braga, Portugal. Recientemente aprobado por el Ministerio de Ciencia Tecnología e Innovación Productiva (Mincyt). Y por el Proyecto (P-031516.) de Investigación: *"Ingeniería de Software: Conceptos, Prácticas y Herramientas para el Desarrollo de Software con Calidad"* de la Facultad de Ciencias Físico Matemáticas y Naturales, Universidad Nacional de San Luis. Dicho proyecto es la continuación de diferentes proyectos de investigación a través de los cuales se ha logrado un importante vínculo con distintas universidades a nivel nacional e internacional. Además, se encuentra reconocido por el Programa de Incentivos.

1. INTRODUCCIÓN

Denning [1] definió la seguridad de los datos como la ciencia que estudia métodos de protección de datos en los sistemas de red, e incluye controles criptográficos, controles de acceso, controles de flujo de información, controles de inferencia y procedimientos para respaldo y seguridad. La seguridad en sistemas basados en IoT implica no sólo proteger datos, claves criptográficas y credenciales. Es por esto, que estos sistemas son propensos a un amplio abanico de amenazas y desafíos en cuanto a la seguridad.

En IoT, los objetos físicos como por ejemplo automóviles, televisores, aires acondicionados, etc. que nos rodean son identificables de forma única y están interconectados [2]. A través de la red de comunicación los objetos se conectan entre sí recolectando información útil entre ellos. La información es transmitida a los diferentes dispositivos que tomarán acción ejecutando una tarea.

Debido a la aceptación de la incorporación de estos dispositivos integrados interconectados en la sociedad, se espera que para el 2020 [3] existan alrededor de 25 mil millones de objetos interconectados en la red mundial. En este marco, surgen amenazas de seguridad y privacidad poniendo a todos esos dispositivos en alto riesgo de vulnerabilidad, haciendo que dichos dispositivos funcionen beneficiando a los atacantes y no para el fin que se espera sean utilizados. Por esto, esta línea de investigación se centra en detectar, encontrar y proponer soluciones que sean adecuadas para reducir las amenazas que estos dispositivos pueden sufrir debido a su fácil acceso y manipulación [4]. Analizar y garantizar la seguridad en los dispositivos es una tarea prioritaria ya que los mismos tienen un impacto directo en la vida de los usuarios pudiendo invadir su privacidad. Para llevar adelante esta tarea, se requiere analizar y

garantizar la existencia de una infraestructura de seguridad correctamente definida, protocolos que limiten las posibles amenazas relacionadas con la escalabilidad, disponibilidad y seguridad en IoT [5].

La línea de investigación comprende los principales lineamientos de:

- Seguridad: Se centra en el estudio de los ejes fundamentales de la seguridad en IoT.
- Arquitectura: Se estudia cada capa y las problemática de la seguridad que pueden ocurrir en dichas capas.
- Modelos de Seguridad: Se estudian diferentes modelos de seguridad que permiten contrarrestar las vulnerabilidades producidas en la diversidad de dispositivos en el mercado de IoT.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

2.1 Seguridad en IoT

Los principales objetivos de seguridad en IoT son garantizar mecanismos de autenticación de identidad adecuados y proporcionar confidencialidad sobre los datos. Un modelo conocido para desarrollar mecanismos de seguridad en IoT se basa en tres áreas:

- **Confidencialidad de Datos:** Es la capacidad de proporcionar confianza y tranquilidad al usuario sobre la privacidad y confidencialidad de sus datos los cuales deben estar protegidos en su totalidad. Para esto se utiliza los mecanismos como el de cifrado de datos, verificación de dos pasos, entre otros.
- **Integridad de Datos:** Se refiere a la protección de datos relevantes, de hackers o de interferencias externas que se pueden producir durante la transmisión y recepción de datos que impide ser manipulados a menos que se detecte la amenaza a tiempo [7]. El Checksum y Cyclic Redundancy Check (CRC), entre otros, son mecanismos que garantizan esta actividad.
- **Disponibilidad de Datos**: Garantiza el acceso inmediato a sus recursos de información a la parte autorizada no sólo en condiciones normales sino también en condiciones adversas. Métodos de copia de seguridad de redundancia y conmutación por error que proporcionan la duplicación de los componentes del sistema en condiciones de falla del sistema o diversos conflictos del sistema que garantizan la fiabilidad y disponibilidad de los datos.

2.2 Arquitectura en IoT

En la Figura Nº 1 se observa la arquitectura general de IoT que está compuesta por cuatro capas.

Figura Nº1 Arquitectura general de IoT

A continuación se describen las diferentes partes que componen la arquitectura de IoT.

- Capa de Percepción (CP): Realiza la identificación de objetos. Recompila datos a través de sus sensores [7]. La seguridad se ve afectada debido a los sensores empleados en esta capa de percepción que son, generalmente, de diferentes tecnologías, por ejemplo los sensores RFID los cuales están expuesto a amenazas de:

  Etiquetas: La falta de un mecanismo de autentificación adecuado en la mayoría de los RFID, permite el acceso de etiquetas sin estar autorizados. Lo que permite realizar lecturas, modificaciones e eliminaciones de datos [8].

  Clonación de Etiquetas: Se crea una réplica de la etiqueta y se compromete

de manera tal que lector no pueda distinguirla de la etiqueta original [9].

Spoofing: Se difunde información falsa en los RFID haciendo parecer que la fuente es original [10]. De esta forma el sistema se vuelve vulnerable.

- Capa de Red: Transmite datos obtenidos de la capa de percepción a través de Internet, red móvil o cualquier otro tipo de red de comunicación confiable [11]. Las problemáticas de en la capa se red son:

  Ataque Sybil: A un único nodo se le da múltiples identidades. Esto hace que el sistema de cómo resultado información incorrecta [12].

  Ataque de Privación de Sueño: Mantiene a los nodos encendidos agotando la batería lo que lleva a que los nodos se apaguen [13].

  Inyección de Código: Se inyecta código malicioso en un nodo. Esto podría provocar tener el control de la red [14].
- Capa de Nivel Medio: Es la encargada de garantizar el mismo tipo de servicio entre los objetos físicos conectados [15]. Los problemas de seguridad se producen en el canal de comunicación. Problemas de:

  Acceso no Autorizado: Podría ser fatal para el sistema ya que el atacante puede prohibir el acceso a servicios relacionados de IoT, o incluido eliminar datos sensibles del sistema.

  Ataque DoS: Ocasiona el apagado del sistema haciendo que los servicios no se encuentren disponibles.
- Capa de Aplicación: Es la encargada de las aplicaciones de IoT provenientes de los más diversos tipos de industrias, como por ejemplo, Smart Hospital, Smart City, Smart Transportation, entre otros [16]. La seguridad de esta capa se encuentra afectada por:

  Inyección de código malicioso: Inyectar código malicioso en el sistema para robar algún tipo de información.

  Ataque de denegación de servicio (DoS): Intenta romper el sistema defensivo y por lo tanto la privacidad de los datos del usuario, mientras engaña a la víctima haciéndole creer que el ataque real está sucediendo en otro lugar.

  Ataque de Spear-Phishing: Suplanta el correo electrónico en el que la víctima, una persona de alto rango, es atraída a abrir el correo electrónico a través del cual el adversario obtiene acceso a las credenciales de esa víctima y luego, con un pretexto, recupera información más confidencial.

2.3 Modelos de Seguridad en IoT

La seguridad del software es la ciencia y el estudio de la protección de software (incluyendo datos de software) contra el acceso no autorizado [17, 18, 19]. Existe diversos principios, enfoques y técnicas para mejorar la seguridad del software de amenazas como, por ejemplo, ataques de overflow de buffer [20], ingeniería inversa y alteración [21], entre otros [22]. Existen modelos que permiten contrarrestar e identificar las amenazas:

- **Modelo de Amenaza de Red:** El atacante intenta obtener acceso privilegiado que le permita realizar acciones maliciosas [23, 24, 25, 26, 27] como, por ejemplo lanzar otros ataques, consumir recursos o recolectar información.
- **Modelo de amenaza interna:** El hacker cuenta con algún nivel de privilegios ya sea en la red o en hardware que ejecuta la aplicación de destino. Esto le permite obtener acceso a datos sensibles los cuales puede alterar y/o realizar un hurto de los mismos.
- **Modelo de amenaza de host no confiable:** El hacker es local y cuenta con todos los privilegios. El hacker puede eliminar restricciones que hubieran hecho para que que el sistema se encuentre en un estado estable, eliminar la protección contra copia, hurto de información relevante, manipular la licencia de datos o de la aplicación.

3. RESULTADOS OBTENIDOS/ESPERADOS

El trabajo de investigación de esta línea permitió obtener los siguientes resultados:

- A partir del estudio y análisis de los dispositivos digitales basados en la tecnología IoT se detectó diversas vulnerabilidades que pueden ser contrarrestadas utilizando métodos técnicas y herramientas centradas en la seguridad de los dispositivos.

- El estudio de la arquitectura de IoT permitió determinar las amenazas (perdida de datos, manipulación de datos, perdida de privacidad, etc.) producidas en cada capa. A fin de reducir estas inseguridades deben ser consideradas en los dispositivos IoT.

- Se determinó la existencia de diferentes modelos para detectar amenazas que permiten contrarrestar la seguridad de software.

Los investigadores de esta línea pretenden a través de investigaciones sustanciales sobre medidas de privacidad y seguridad, evoluciones de riesgo, arquitectura, problemas de autentificación, entre otros, proporcionar respuestas a problemas abiertos en este campo del Internet of Things antes de que sean implementados e incorporados a la sociedad. Así como desarrollar métodos, técnicas y herramientas que ayuden, en un mayor grado, al desarrollo estable de tecnologías seguras en este campo de investigación tan amplio del Internet of Things.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo de profesionales de la UNSL que forman parte de la línea de investigación de este trabajo llevan adelante diferentes trabajos finales integradores de *Ingeniería en Informática, Ingeniería en Computación, Licenciatura en Ciencias de la Computación*, y en un futuro próximo trabajos finales de especialización, tesis de maestría y doctorado. En particular, las investigaciones desarrolladas en este trabajo forman parte del lineamiento inicial de una tesis doctoral de uno de los autores para optar al grado de Doctor en Ingeniería en Informática en la UNSL.

5. BIBLIOGRAFÍA

[1] D. Denning, Cryptography and Data Security, Addison Wesley, 1982

[2] D. Singh, G. Tripathi, A.J. Jara, A survey of Internet of Things: Future Vision, Architecture, Challenges and Services, in Internet of Things (WF-IoT), 2014

[3] Gartner, Inc. It can be accessed at: http://www.-gartner.com/newsroom/id/2905717

[4] Rodrigo Roman, Pablo Najera and Javier Lopez, ”Securing the Internet of Things,” in IEEE Computer, Volume 44, Number 9, 2011, pp. 51-58

[5] Friedemann Mattern and Christian Floerkemeier, ”From the Internet of Computers to the Internet of Things,” in Lecture Notes In Computer Science (LNCS), Volume 6462, 2010, pp 242-259

[6] Luigi Atzori, Antonio Iera, Giacomo Morabito, ”The Internet of Things: A Survey,” in Computer Networks, pp. 2787-2805

[7] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in Electrical and Control Engineering (ICECE), pp. 4109-4112

[8] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, ”Internet of Things: Architecture and Security,” in International Journal of Computer Application, Volume 3, Issue 4, 2014

[9] Mike Burmester and Breno de Medeiros, ”RFID Security: Attacks, Countermeasures and Challenges.”

[10] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, ”Classification of RFID Attacks.”

[11] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multilayer Security Model for Internet of Things, in Communications in Computer and

Information Science, 2012, Volume 312, pp 388-393.

[12] John R. Douceur, ”The Sybil Attack,” in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260

[13] Tapalina Bhattasali, Rituparna Chaki and Sugata Sanyal, ”Sleep Deprivation Attack Detection in Wireless Sensor Network,” in International Journal of Computer Applications, Volume 40, Number 15, 2012

[14] Priyanka S. Fulare and Nikita Chavhan, ”False Data Detection in Wireless Sensor Network with Secure Communication,” in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1, 2011

[15] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[16] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[17] J. Viega, G. McGraw, Building Secure Software, Addison Wesley, 2001

[18] M. Howard, D.C. LeBlanc, Writing Secure Code, 2nd ed., Microsoft Press, 2002

[19] P.C. van Oorschot, “Revisiting Software Protection”, pp.1–13, Proc. of 6th International Information Security Conference (ISC 2003), Bristol, UK, October 2003, Springer-Verlag LNCS 2851 (2003)

[20] J. Wilander, M. Kamkar, “A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention”, pp.149-162, Proc. of NDSS’03 (Internet Society): Network and Distributed System Security Symp., Feb. 2003, San Diego.

[21] J. Gosler, “Software Protection: Myth or Reality?”, Advances in Cryptology – CRYPTO’85, Springer-Verlag LNCS 218 (1985), pp.140–157

[22] L. D’Anna, B. Matt, A. Reisse, T. Van Vleck, S. Schwab, P. LeBlanc, “Self- Protecting Mobile Agents Obfuscation Report”, Network Associates Labs Report #03-015, 30 June 2003

[23] CERT Advisory CA-1996-26 Denial-of-Service Attack via ping (“Ping of Death”), http://www.cert.org/advisories/CA-1996-26.html, accessed 29 Dec. 2003

[24] D. Bleichenbacher, “Chosen Ciphertext Attacks against Protocols Based on RSA Encryption Standard PKCS #1”, Advances in Cryptology – CRYPTO’98

[25] D.M. Kienzle, M.C. Elder, “Recent Worms: A Survey and Trends”, pp.1-10

[26] N. Weaver, V. Paxson, S. Staniford, R. Cunningham, “A Taxonomy of Computer Worms”, pp.11–18

[27] Symantec, “What is the difference between viruses, worms, and Trojans?”, http://service1.symantec.-com/SUPPORT/nav.nsf/pfdocs/199904120913110 6, October 1 2003